

至高のセキュリティ **ISPX Track Express**  
指紋認証 & パスワード認証 & 利用PC限定の3段階認証



ご紹介資料

エムコマース株式会社

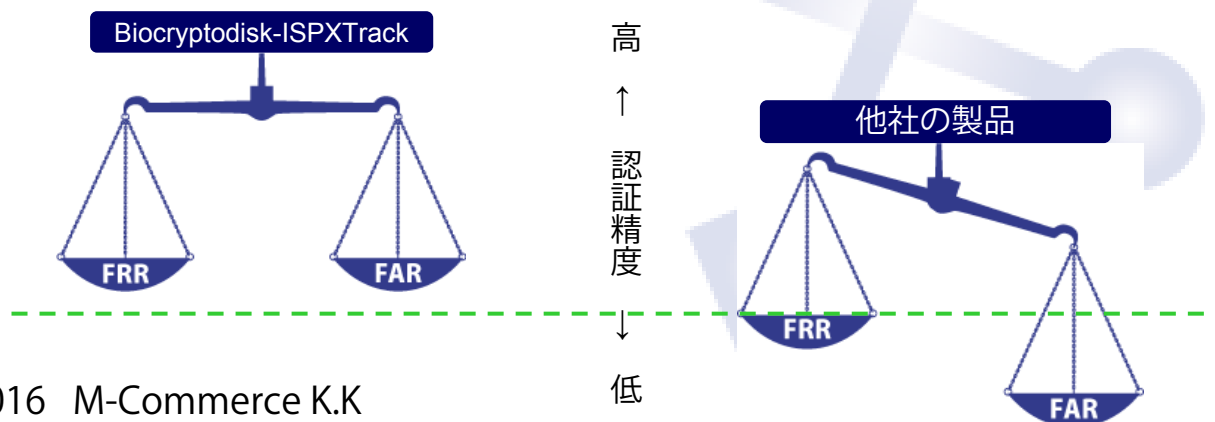
▶情報漏洩は外的要因と内的要因から起きています。

	外的要因	内的要因
情報漏洩	盗難・紛失 紛失時の内部データ・パスワード解析 ウィルスの侵入	データの無断持ち出し パスワードの漏洩 悪用、無許可PCでの不正使用 (自宅、ネットカフェ等)
対策	会社選定のUSBメモリを貸与 保存データの暗号化 生体認証の採用 ウィルス対策 デバイス制御	セキュリティポリシーの徹底
効果・問題点	安全面で最善をつくした施策を行える。 安全面が優先になり、操作性、利便性がそこなわれてしまいがちになる。	操作性、利便性が優先され、遵守されない場合がある。 不正使用をしても発覚しないと思っている。 懲戒処分は免れない。

➤ 認証精度を表す数値（数値が小さいほど精度が高い）

<p><b>本人拒否率</b> (FRR : False Rejection Rate) 本人を誤って拒否してしまう確率</p>	<p>他人を拒否する精度が高まる一方、 本人も拒否しやすくなり、 使い勝手が悪くなる。</p>
<p><b>他人受入率</b> (FAR : False Acceptance Rate) 他人を誤って受け入れてしまう確率</p>	<p>本人を受け入れやすくする一方、 他人も受け入れやすくなり、 安全性が失われる。</p>

➤ 本人拒否率と他人受入率それぞれ独立した値ではなく、相関関係を持っています。  
 「セキュリティレベルが高い」とは、  
 数値が小さく、かつ両方の数値のバランスがとれていることを示します。



エムコマースの指紋認証は、指紋の切れ目（端点）や分かれ目（分岐点）などの特徴点を相対座標データとして抽出し、登録されている特徴点データと照合することで実現しています。（特徴点抽出方式）

エムコマースの認証精度向上のしくみは、**独自の画像エンハンスメント**。センサより得られた指紋画像が認証に不十分なレベルであったとしても、2値化画像を作成する際の最適化技術や、指紋取り込み条件の自動化処理等、エムコマース独自の画像エンハンスメント処理で、認証に十分なレベルに引き上げます。これにより難指紋への対応が強化され、対応率も大幅に増加しました。

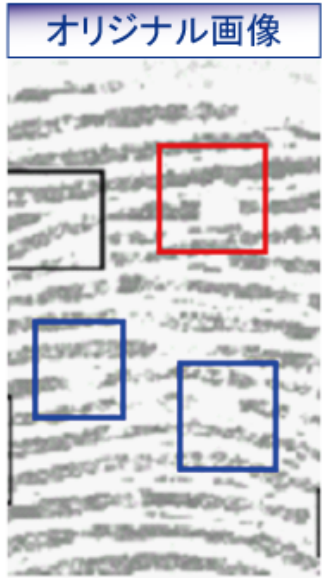
## Image enhancement



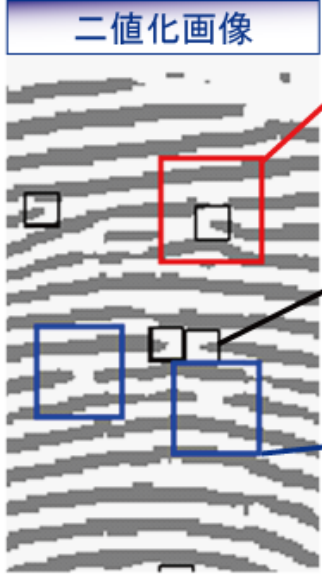
**ワンポイント)** 二値化とは黒と白の2色ではっきりとした画像に処理することです。この際にノイズの除去を同時に行います。この作業が特徴点抽出には不可欠です。

## 画像エンハンスメント例

オリジナル画像



二値化画像

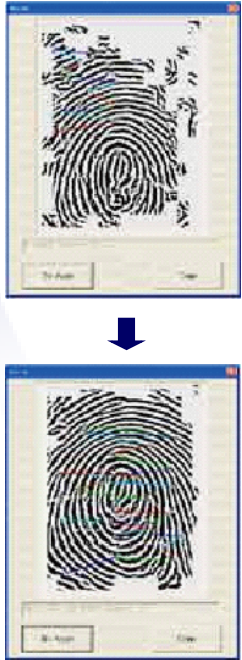


**赤枠の部分は分岐点と判断する**  
オリジナル画像では見えにくい部分ですが、過程2の配置において画像を修復して分岐点であることを認識しています。

**黒枠の部分は分岐点と判断する**  
オリジナル画像でも二値化画像でも切れています。過程2の配置において端点であることを認識しています。

**青枠の部分は特徴点と判断しない**  
オリジナル画像でも二値化画像でも切れているように見えますが、過程2の配置において特徴点でないことを認識しています。

指紋の欠損部を修復します。



読み取った画像をなるべく補正し、認証に適切な状態で登録することで画像に多少の欠損があってもスムーズで確実な認証が行えます。何度も本人認証に失敗する（本人拒否）ストレスは、この技術の差に起因します。エムコマースは、独自の画像エンハンスメント技術により、7万分の4の本人拒否率を実現しています。



# それでも情報漏洩は起こっています

- ▶ 個人所有PCなど管理外のPCを利用できる環境が、管理者を悩ませています。
- ▶ マイナンバー管理を含む最近の情報管理ポリシーにおいて「2段階以上の認証」が求められています。

- ☑ 社内のPCにはデバイス制御とウイルス対策
- ☑ 従業者にはセキュリティ対策USBメモリを貸与

- ☑ 装置側の施策で情報漏洩を防止
- ☑ 情報セキュリティポリシーの徹底



☑ 許可された人 + ☑ 許可されたデバイス =

それでも情報漏洩?!

## ▶利用したPCの履歴情報（ログ）の説明

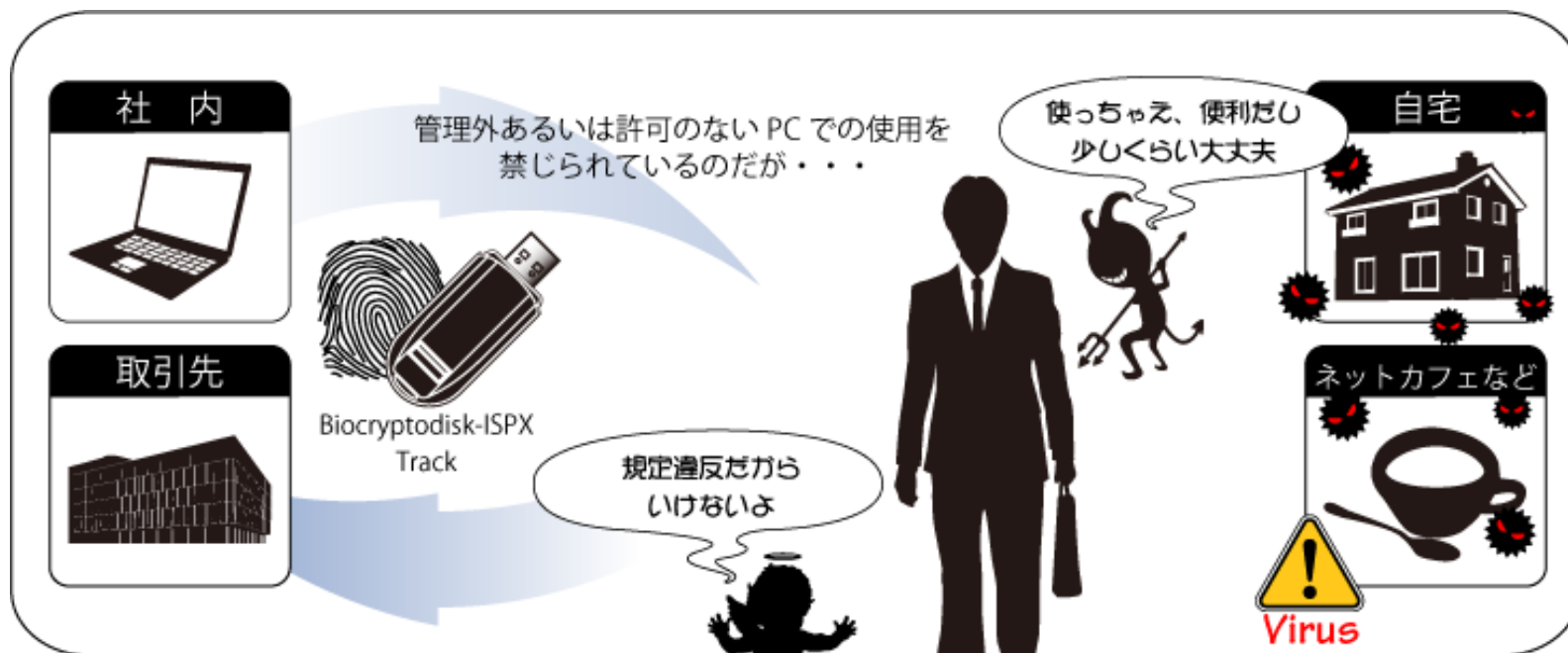
- ▶履歴情報（ログ）はメモリドライブとは別の秘匿領域に自動記録されます。
- ▶一般利用者がフラッシュドライブをフォーマットしてもログは消えません。
- ▶ログの閲覧ツールは、一般利用者には提供されません。
- ▶ログは最新の1,000件（最大）が格納されます。
- ▶ログ情報をCSVファイルへ出力可能です。

No.	ユーザー名	コンピュータ名	PCシリアル	HDD ID	利用日時
44	shain_c	DELL3100C	CN7082161C0	BFEBFBFF0000F49	2012-10-16/11-59-30
45	bucho	INSPIRON1	B8HG7BX CN4	078BFBF00040FC2	2012-09-24/17-19-15
46	shain_c	DELL3100C	CN7082161C0	BFEBFBFF0000F49	2012-07-09/14-45-32
47	shain_c	DELL3100C	CN7082161C0	BFEBFBFF0000F49	2012-06-25/10-45-42
48	kscho	DELL3100C	CN4	078BFBF00040FC2	2012-06-25/10-44-22
49	shain_a	DELL3100C	CN48	078BFBF00040FC2	2012-06-25/10-42-20
50	shain_a	DELL3100C	CN48	078BFBF00040FC2	2012-06-22/10-06-55
51	shain_b	VOSTRO764	CN48	BFEBFBFF000206A7	2012-06-21/12-29-49
52	shain_a	DELL3100C	CN48	078BFBF00040FC2	2012-06-20/09-35-48
53	shain_b	DELL3100C	CN7082161C0	BFEBFBFF0000F49	2012-06-20/09-31-06
54	shain_d	DELL3100C	11374077100	078BFBF00050FF2	2012-06-07/15-26-16
55	shain_c	DELL3100C	CN7082161C0	BFEBFBFF0000F49	2012-06-07/15-21-33
56	shain_b	DELL3100C	CN7082161C0	BFEBFBFF0000F49	2012-06-07/12-43-35

ログには次の情報が含まれます。

- ① ISPX Track Express 固体情報
- ② ユーザー名
- ③ 使用したコンピュータ名
- ④ PCのシリアル番号
- ⑤ PCのCPU ID
- ⑥ PCのHDD ID
- ⑦ 利用日時

管理外の PC ?!



利用履歴は自動記録され  
 使用したPCの追跡が可能。  
 ログ機能を周知し  
 定期的な監査を行うことにより  
 『不正使用に対する抑止効果』が生まれる。

**Track** (追跡)

User PCname Serial Number  
 CPUID HDID Date&Time

User	PCname	Serial Number	CPUID	HDID	Date&Time
user_1	DELLI PC	0A702 M1C3	87C8F9F0000F48	33D-531-671-48-30	
user_2	ASUSC23	89C231 04	0589F11888F12	33D-06-267-38-35	
user_3	DELLI PC	0A702 M1C3	87C8F9F0000F48	33D-0F-8874-42-32	
user_4	DELLI PC	0A702 M1C3	87C8F9F0000F48	33D-06-267-44-43	
user_5	ASUSC23	89C231 04	0589F11888F12	33D-06-267-44-43	
user_6	DELLI PC	0A702 M1C3	87C8F9F0000F48	33D-06-267-42-30	
user_7	ASUSC23	89C231 04	0589F11888F12	33D-06-267-44-43	
user_8	DELLI PC	0A702 M1C3	87C8F9F0000F48	33D-06-267-42-30	
user_9	DELLI PC	0A702 M1C3	87C8F9F0000F48	33D-06-267-42-30	
user_10	DELLI PC	0A702 M1C3	87C8F9F0000F48	33D-06-267-42-30	

管理外のPC?!



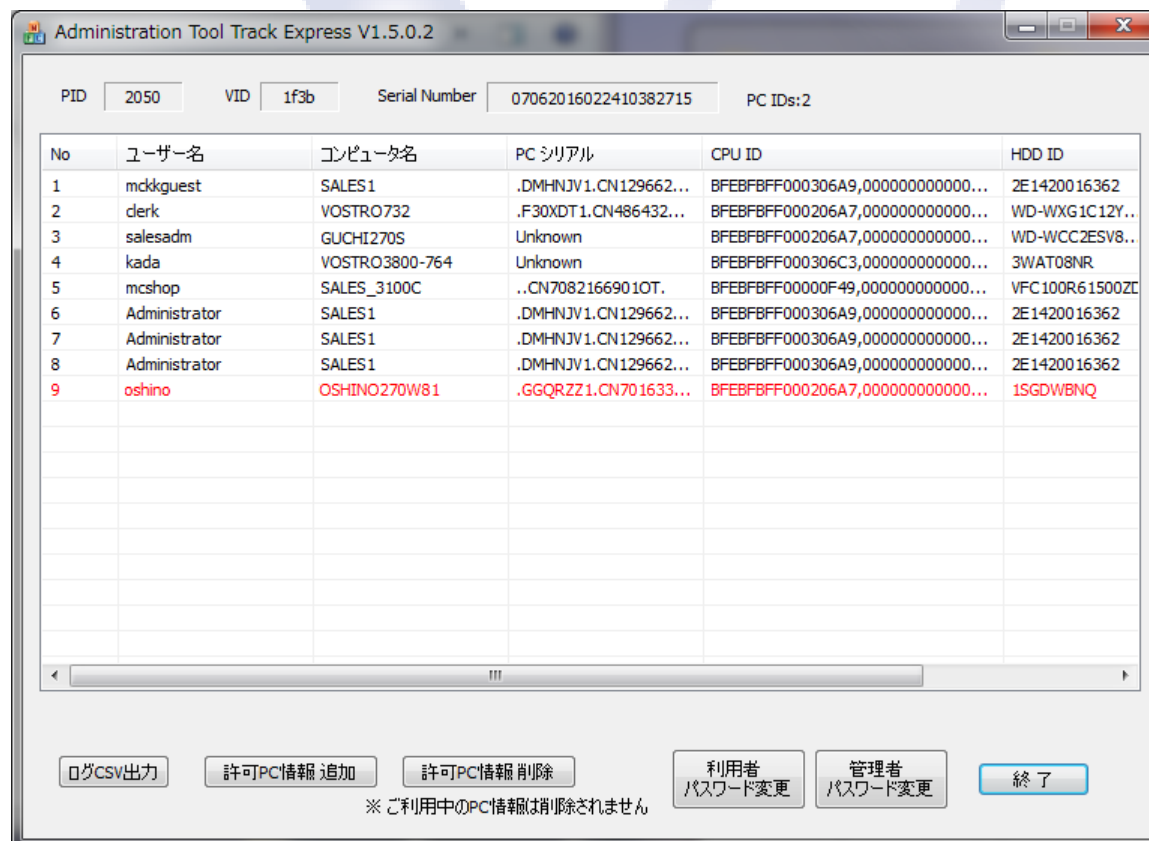
- **指紋認証 & パスワード認証 & 利用PC限定の3段階認証**  
指紋認証 & パスワード認証 & 利用PC限定の3段階認証用を必須とした至高のセキュリティUSBメモリです。
- **使用したPCの履歴情報を自動記録**  
使用したPCの履歴情報を自動記録することで、利用者のセキュリティポリシーに対する意識が高まります。
- **利用PC限定機能を標準搭載**  
以前の製品でオプション機能として提供していた利用PC限定機能を標準搭載しました。
- **指紋認証以外のバックドア（抜け道）は、一切なし**  
指紋認証以外では、全メモリ領域の参照はできません。
- **AES-256 自動暗号化機能搭載！ 512Bごとに独立した鍵で暗号化**  
メモリ内に保存される全てのデータは自動的に暗号化されます。
- **最高水準の認証精度**  
本人拒否率0.05%、他人受入率0.0001%、認証時間は0.6秒です。
- **専用ソフト・ドライバーのインストールが不要だから幅広いOSに対応**  
Windows 10 / 8.1 / 8 / 7 / Vista 対応。
- **機器内指紋認証（インテリジェントタイプ）**  
ハッキングの対象となる指紋情報や認証信号も機器内から漏出しません。

Biocryptodisk-ISPXシリーズは、紛失や盗難などによって分解されても参照できない物理的な対策がとられています。  
バックドアがあったり、認証精度の良くない製品ではセキュリティ対策の意味がありません。

**絶対的な安全性で選んでください。**

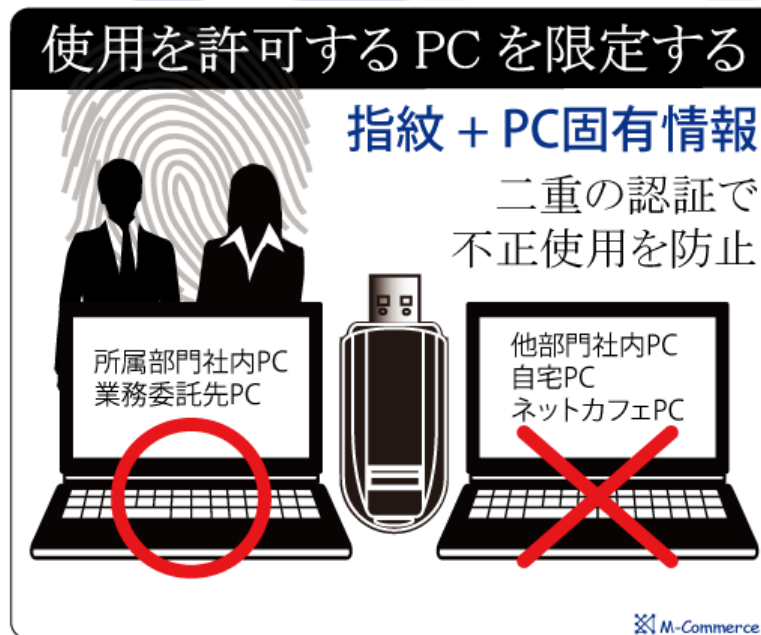
## ➤ 利用したPCの履歴情報を自動記録

ISPX Track Expressは、USBメモリの不正利用という問題点に着目し、使用したPCの履歴情報を自動記録することで利用者のセキュリティポリシーに対する意識を高める、指紋認証USBメモリです。本人拒否率0.05%の認証精度を誇る「Biocryptodisk-ISPX」の基本技術を応用、利用履歴を記録する機能は機器内に搭載されており、専用ソフトをインストールする必要はありません。



利用を許可するPCの固有情報をISPX Track Expressに登録し許可されたPC以外での不正使用を禁止する機能です

- 使用を許可しないパソコンではISPX Track Expressを接続しても一切のデータの読み書きを行うことができません。
- ファイル共有ソフト (Winny等)からの情報漏洩も防止できます。
- USBメモリ経由でのウィルス感染のリスクを回避する事ができます。



## ➤指紋認証以外のバックドア（抜け道）は、一切なし

データの参照は指紋認証に限定。

パスワード認証を代替にすると、「なりすまし」による不正使用や悪用の抜け道ができてしまうのです。

精度の高い指紋認証の技術があればこそ実現できる、ストレスのない絶対の安全性です。



## ➤AES-256 自動暗号化機能搭載！ 512Bごとに独立した鍵で暗号化

内部データは、指紋情報やアプリケーションデータを含め、全て自動で高いレベル（AES-256）で暗号化され保存されます。さらに、単一ではなく512Bごとに自動生成された個別の暗号鍵を使用し、暗号化されます。

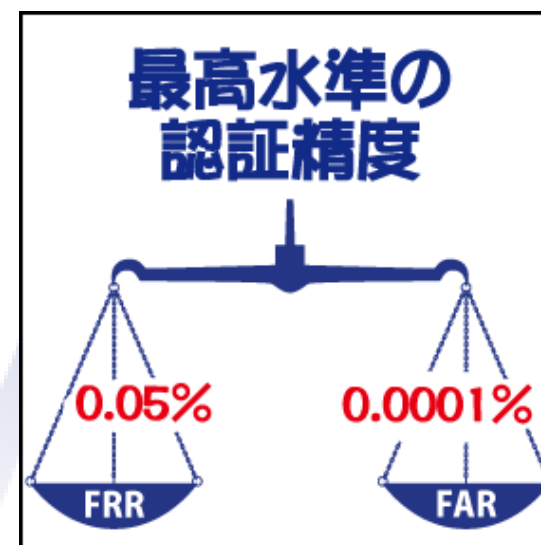


## ▶ 最高水準の認証精度

認証速度は、平均わずか0.6秒。

速さに加え、**本人拒否率は0.05%**で、累計70,000人中なんと4人。**他人受入率は0.0001%**と、**きわめて高い認証制度を誇ります。**

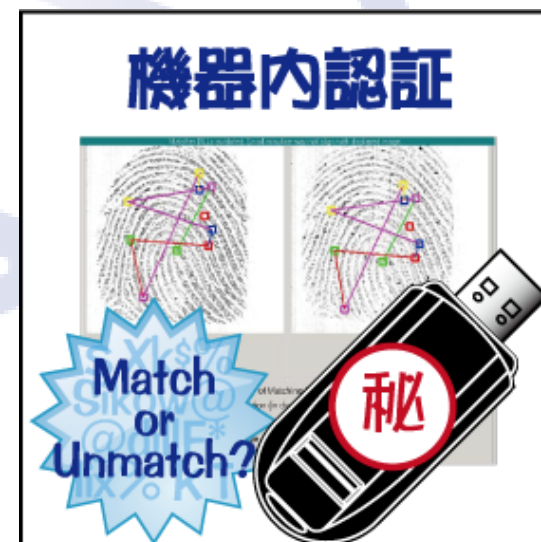
指紋認証はみな同じではありません。認証精度で選んでください。



## ▶ 機器内指紋認証 (インテリジェントタイプ)

指紋情報は画像データではなく特徴点の座標情報を機器内の高度な秘匿エリアに暗号化して格納。外部からの読み出しは一切不可能です。

PC内認証タイプは、指紋認証機器とPC間で特徴点などの指紋情報や認証した結果の合否の通信が行われますが、この通信もハッキングのリスクがあります。





製品型番	HKISK-08-4X (JANコード: 4582420180129)
メモリ容量	8 GB (AES-256自動暗号化機能搭載)
転送速度	最大18MB/秒 (書込み時)、24MB/秒 (読出し時)
指紋センサ	静電容量式半導体センサ
解像度	508dpi
登録指紋数	6指 (管理者2指+ユーザ4指)
インタフェース	USB1.1/2.0 (バスパワー)
対応OS	Windows 10 / 8.1 / 8 / 7 / Vista
動作温度	5°C~55°C、最大85%RH (結露無きこと)
保存温度	-20°C~65°C、最大85%RH (結露無きこと)



マイナンバー  
管理に最適

Windows 10 / 8.1 対応!!

指紋&パスワード認証  
& 利用PC限定

指紋認証USBメモリ  
**ISPX Track Express**  
アイエスピーエクストラックエクスプレス